REVISTA de la Facultad de Ciencias Jurídicas y Sociales

Nueva Época
Publicación anual / número 14 / año 2025
ISSN 2362-3306 / **DOI** 10.14409/e1004
Universidad Nacional del Litoral, Argentina

Protección de datos personales: El futuro llegó, hace rato

Personal data protección: The future arrived a while ago

Hernán G. Gálvez
hernangalvez@outlook.com.ar
Universidad Nacional del Litoral, Argentina

Resumen: El presente trabajo trata sobre la importancia actual que reviste la defensa del derecho personalísimo al dato personal como integrante del núcleo de derechos humanos fundamentales, en el contexto de la evolución vertiginosa de las nuevas tecnologías de recolección, tratamiento y transmisión de metadatos.

Palabras clave: Derechos personalísimos al dato personal, medios de protección, nuevas tecnologías, metadatos, derechos del consumidor.

Summary: *This paper addresses the current importance of defending right to personal data as part of the core of fundamental human rights, in the context of the rapid development of new technologies for collecting, processing, and transmitting metadata.*

Keywords: *Personal Data Rights, means of protección, new techs, metadata, consumer rights.*

1. Introducción

Hace unos pocos días, se cumplieron diez años de la puesta en vigencia del Código Civil y Comercial de la Nación.

Entre sus novedades se destaca la regulación expresa de los derechos personalísimos en sus distintas manifestaciones (Conf, art. 52, 53 y ss CCCN), inscribiéndose dentro de una protección genérica contra todo menoscabo de la dignidad personal como derecho humano fundamental (art. 51 CCCN).

En una de las tantas presentaciones del CCCN a las que asistí en nuestra Facultad de Ciencias Juridicas y Sociales de la Universidad Nacional del Litoral, uno de sus redactores, el Dr. Ricardo Lorenzetti recalcó que el nuevo Código es un código para las generaciones presentes, pero fundamentalmente, para las generaciones futuras, las que debido a los adelantos tecnológicos en distintas disciplinas (salud, comunicaciones, etc) verían en riesgo sistemático sus derechos personalísimos.

Recuerdo también que exponía como ejemplo de ello, personas en situación de vulnerabilidad económica que podrían llegar a consentir un tratamiento médico experimental riesgoso para su integridad física y la protección que el artículo 58 del CCCN les dispensaría en aquellas situaciones.

Supongo que la mayoría de los que estábamos presentes en ese auditorio no imaginó ni por un minuto que aquel mundo lejano —distópico para muchos— se iba a presentar tan rápido ante los ojos de la humanidad.

Nuestra vida cotidiana desde hace unos años transcurre en ámbitos digitales y nuestras huellas son almacenadas y procesadas continuamente. Esa capacidad de procesamiento, se ve actualmente potenciada por la IA, que puede generar nueva información a partir de la ya disponible, permitiendo la creación de perfiles, la predicción de comportamientos, etc.

Como reza aquella celebre canción del rock nacional, el futuro llegó, hace rato.[1]

[1] La frase pertenece a la canción "todo un palo" de los Redonditos de Ricota.

Para citar este artículo: Gálvez, H. G. (2025). Protección de datos personales: El futuro llegó, hace rato. *Nueva Época, Revista de la Facultad de Ciencias Jurídicas y Sociales. Num. 14*, e1004. DOI: 10.14409/e1004

Publicación de acceso abierto bajo licencia Creative Commons Atribución-NoComercial-CompartirIgual 4.0 Internacional

2. El derecho al dato personal: un derecho constantemente acechado

En hechos relativamente recientes, vemos como los datos personales son objeto de ataques bajo distintas modalidades y para distintos fines.

Una de las finalidades para las que se recopilan datos es el denominado control social o vigilancia masiva.

Citemos algunos ejemplos.

Corría el año 2013 cuando Edward Snowden revelaba como la Agencia de Seguridad Norteamericana (NSA) había accedido a las bases de datos de Google y Facebook y había interceptado conversaciones de personas de todo el mundo, incluyendo de lideres políticos, había recopilado datos, llamadas, conversaciones en línea de todo tipo, ocurridas dentro del ecosistema de redes de telecomunicaciones. [2]

El caso Snowden expuso frente al mundo la vulnerabilidad de los datos recopilados por estas grandes empresas tecnológicas y como podía llevarse adelante —sea por la misma empresa o por un gobierno, como en este caso— un programa de vigilancia masiva a través de los datos personales.

En 2022, en el marco de un amparo colectivo, se declaró la inconstitucionalidad de la Resolución 398/19 —Sistema de Reconocimiento Facial de Prófugos (SRFP)— que en el ámbito de la Ciudad de Buenos Aires puso en marcha desde el año 2019 un programa de reconocimiento facial para monitorear el acceso a espacios públicos y privados sirviéndose de bases de datos biométricos del RENAPER.

Como en sistemas análogos de países europeos, la finalidad de dicho programa era la búsqueda de cuarenta mil prófugos de la justicia, pero en la causa se terminó probando que se recabaron los datos de mas de diez millones de personas cuyo paradero no había sido solicitado, por lo que además de la declaración de inconstitucionalidad por la flagrante violación de los datos personales, se mandó a destruir la base de datos biométricos y los registros creados a tales fines de todas aquellas personas que no tenían abierta causa judicial alguna u orden judicial a tal efecto. [3]

En el mes de junio de 2024 la Sala V de la Cámara Nacional de Apelaciones en lo Contencioso Administrativo Federal, en el marco de un habeas data colectivo e identificando los derechos en pugna como de incidencia colectiva, declaró la inconstitucionalidad del artículo 1° de la Decisión Administrativa de Jefatura de Gabinete de la Nación 431/2020, que habilitaba la transferencia entre organismos públicos de datos personales recabados durante la emergencia sanitaria por COVID-19, sin previo consentimiento de los titulares, y del art. 5 inc. 2 b) de la Ley 25.326 de Protección de Datos Personales que lo permite. Además, se ordenó al Estado Nacional cesar con la recopilación, transmisión y tratamiento de esos datos personales que excedan los consentimientos dados por los titulares al momento de su recolección, así como eliminarlos de sus sistemas.

La recopilación y análisis de datos personales también persigue la creación de perfiles de individuos o grupos sociales para destinarlos a distintas actividades lucrativas.

Así, los metadatos son activos intangibles que las grandes empresas utilizan para identificar patrones de consumo y direccionar de este modo la actividad publicitaria o, incluso, para hacer targeting o microtargeting y así identificar preferencias políticas.

La fundación Worldcoin, especializada en la verificación de identidad a través del escaneo facial y del iris, celebró millones de contratos en distintos países —incluido el nuestro— para la obtención de datos biométricos a cambio de una compensación económica en criptomonedas. La finalidad que se describió en el contrato fue la de la creación de una identidad digital.

La actividad de la fundación se encuentra bajo investigación en el país[4] por parte de la Agencia de Acceso a la Información Pública (AAIP) dado que han surgido distintos cuestionamientos sobre el consentimiento

---

[2] A raíz del caso Snowden en el año 2018, la Unión Europea puso en marcha el Reglamento General de Protección de Datos (RGPD), con el objetivo de limitar las posibilidades de que empresas estadounidenses como Google o Facebook colecten y hagan un uso libre de los datos de los usuarios.

[3] El amparo fue motorizado por la ONG Observatorio de Derecho Informático Argentino (ODIA). La jueza Elena Liberatore afirmó en su fallo que debía supeditarse la puesta en funcionamiento de este sistema a la ejecución de mecanismos de participación ciudadana y a la realización de un estudio previo relativo al impacto sobre los datos personales, como ya había advertido la Defensoría del Pueblo porteña.

Asimismo, afirmó que el SRFP se implementó sin cumplir con los recaudos legales de protección de los derechos personalísimos de los habitantes de la Ciudad de Buenos Aires. Además, destaca la relevancia de la información provista por la Defensoría del Pueblo, que permitió probar fallas en su funcionamiento "la mera eventualidad de estas falencias con las consecuencias que se derivan en los derechos personalísimos de las personas afectadas y la ausencia de controles –no por no estar contemplados en las leyes sino por la ausencia de debida implementación conforme a ellas–, demuestra un grave grado de riesgo de vulneración de derechos personales".

[4] https://www.argentina.gob.ar/noticias/avanza-la-investigacion-de-la-aaip-sobre-worldcoin-y-el-uso-de-datos-personales.

para el tratamiento de los datos —especialmente en menores—, el destino final de esos datos y su plazo de conservación. Incluso, hay jurisdicciones provinciales en las que ha recibido fuertes sanciones. [5]

No puede dejar de citarse la gran cantidad de hechos ilícitos cometidos por ciberdelincuentes que, sirviéndose de filtraciones de bases de datos personales disponibles en la red, generan perjuicios de todo tipo a los titulares de los datos.

Así, distintas fuentes[6] dan cuenta del crecimiento exponencial de las denominadas estafas virtuales en el ámbito del comercio electrónico, que se desarrollan bajo distintas modalidades.[7] El fraude en línea, la suplantación de identidad, el phishing —sustracción de datos personales— y el acoso virtual o extorsivo son frecuentes.

Por último, cabe mencionar que el uso de la IA generativa es una técnica riesgosa en materia de tratamiento de datos y que hoy se encuentra en pleno auge.

Debe recordarse que el algoritmo es una fórmula para llegar a un determinado resultado. LA IA busca imitar o replicar la forma de aprendizaje automatizado. Se entrena al sistema con datos, cuanto mayor cantidad de datos, mejor trabajará el algoritmo.

Existen determinados lugares en los que el uso de la IA generativa sin control puede derivar en graves violaciones al derecho personalísimo al dato personal.

La justicia es uno de esos espacios. Si se vuelcan datos personales y sensibles de los litigantes a la IA, ese contenido pasa a ser parte de ese aprendizaje automatizado, con capacidad de afectar la privacidad y la identidad misma de la persona.

La introducción de datos personales en la IA generativa, no constituye otra cosa que cesiones de datos de particulares a empresas privadas. Y esas mismas empresas, ceden o comparten datos con otras empresas y con todo aquél con que la empresa se vincule. Por tanto, una vez que salió de la esfera de control de quien lo recabó se hace muy difícil determinar la trazabilidad del dato .

Como se advierte con todos estos ejemplos, y sin pretensión de agotar la cantidad de supuestos —lo cual sería imposible— los ataques al derecho personalísimo al dato personal se encuentran a la orden del día, pueden responder a distintas finalidades y provenir de distintos actores.

3. El derecho personalísimo al dato personal. Generalidades. Derecho con jerarquía constitucional. Ley de Protección de datos personales

Frente a este cuadro variado de situación —que creemos no mejorará, sino todo lo contrario, evolucionará— todo operador jurídico debe conocer los contornos de este derecho, sus alcances y fundamentalmente, las vías o medios de protección.

En primer lugar, el derecho al dato personal pertenece a la categoría de derechos personalísimos de la integridad espiritual y se presenta como un derecho humano fundamental de toda sociedad democrática que pretenda proteger la autonomía de sus ciudadanos.

Creemos con Cifuentes que si bien existen ciertas aristas de este derecho que lo emparentan con la intimidad, con la identidad e incluso con la imagen y que comparten las características de ser esenciales, de objeto interior, necesarios, vitalicios y relativamente indisponibles, lo cierto es que es una categoría autónoma que abarca el derecho a conocer la información que se encuentra en las bases de datos, a rectificarla o corregirla, a actualizarla, a que sea reservada y que no sea utilizada con fines distintos a los invocados cuando fueron recolectados.

Los orígenes de este derecho derivan de la teoría alemana de la autodeterminación informativa,[8] que se concreta en la prerrogativa que todas las personas tienen de ejercer el control sobre su información personal contenida en registros públicos y privados, recolectados y procesados mediante recursos informáticos.

---

[5] https://www.pagina12.com.ar/754648-la-provincia-de-buenos-aires-sanciono-a-worldcoin.

[6] https://www.lanacion.com.ar/seguridad/ciberdelitos-en-alza-record-de-denuncias-whatsapp-como-blanco-principal-y-crecen-los-casos-de-nid30062025/.

[7] https://chequeado.com/el-explicador/las-denuncias-de-estafas-virtuales-aumentaron-un-21-en-2024-cuales-son-los-tipos-de-fraude-mas-comunes/.

[8] El término «autodeterminación informativa» se utilizó por primera vez en el contexto de una sentencia constitucional alemana relativa a la información personal recopilada durante el censo de 1983. El término alemán es informationelle Selbstbestimmung .Se define formalmente como «la facultad del individuo para decidir por sí mismo, basándose en la idea de autodeterminación, cuándo y dentro de qué

Se trata de una fusión entre la autonomía de la voluntad y del derecho a la información: autogobernar nuestros datos personales existentes en distintos registros.

La Corte Suprema de Justicia de los Estados Unidos trató el derecho a la autodeterminación informativa como una evolución del derecho a la intimidad, donde el bien jurídico protegido no era solamente el dato reservado o secreto, sino todo tipo de dato personal.

Por su parte, los estados europeos ya hacía tiempo habían aprobado mediante el Consejo de Europa el Convenio 108[9] para la protección de personas con respecto al tratamiento automatizado de datos de carácter personal.

Dicho convenio[10] estableció distintos principios rectores para la recopilación de datos personales; Finalidad: Los datos personales solo pueden ser recolectados para fines específicos, legítimos y determinados; Adecuación y Pertinencia: Los datos deben ser apropiados, relevantes y no excesivos en relación con las finalidades establecidas; Exactitud y Actualización: Los datos deben ser exactos y mantenerse actualizados; Conservación: Los datos deben ser guardados de forma que permitan identificar a la persona por un tiempo no mayor al necesario para cumplir el propósito original; Seguridad: Se deben implementar medidas de seguridad para proteger los datos contra la destrucción, pérdida o difusión no autorizada; Tratamiento Lícito: Los datos deben obtenerse y usarse de manera legal y legítima.

En nuestro país, la reforma constitucional del año 1994 incorporó al párrafo tercero del artículo 43 la tutela de los datos personales bajo el paraguas de la acción de amparo. Los convencionales constituyentes tuvieron en miras la protección de los particulares frente a la recolección de información de las personas, relativas a su pertenencia política, creencias religiosas, militancia gremial, desempeños en los ámbitos laborales, académicos, estudiantiles, con fines de persecución ideológica, lo que se explica teniendo en cuenta la cercana experiencia en aquel tiempo con la dictadura militar y sus prácticas de identificación de personas con fines de inteligencia o de seguridad nacional.

En el año 2000, luego que se discutiera intensamente en distintos ámbitos académicos la naturaleza jurídica del instituto del habeas data, incorporado al texto constitucional e incluso con pronunciamientos de nuestro más Alto Tribunal,[11] se sancionó la ley 23.526 (LPDP), que vendría a reglamentar el derecho a la protección de datos personales jerarquizado constitucionalmente.

La ley define al dato personal como la información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables.

Siguiendo a Molina Quiroga, la protección del derecho al dato personal en la ley se basa en los principios de calidad de los datos, licitud de la recolección, respeto de la finalidad declarada para la recolección, consentimiento y conocimiento del afectado y existencia de órganos de control independientes.

En efecto, en la sistemática de la ley, la recolección de datos personales encuentra como presupuesto la obtención previa del consentimiento informado del titular de los datos. (Confr. Art. 6 LPDP).

La información con la que el titular del dato debe contar previamente refiere, principlmente, a la finalidad con la que serán tratados los datos y sus destinatarios; la existencia del archivo, registro, banco de datos de que se trate y la identidad y domicilio de su responsable; las consecuencias de proporcionar los datos, de la negativa a hacerlo o de su inexactitud; así como la posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de datos.

No es necesario el consentimiento cuando los datos personales surjan de una fuente de acceso público irrestricto; cuando se recaben como consecuencia del ejercicio de una de las funciones propias de los poderes del estado o en virtud de una obligación legal; cuando se trate de listados cuyos datos se limiten al nombre, DNI, Identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio; cuando deriven de una relación contractual, científica o profesional del titular de los datos y resulten necesarios para su desarrollo o cumplimiento o se trate de las operaciones que realicen las entidades financieras y de las informaciones que reciban de sus clientes conforme lo establecido por el art. 39 de la LPDP.

Asimismo, la LPDP contempla para el titular del dato, el ejercicio de los siguientes derechos: derecho de información y su contenido (Art. 13); derecho de acceso al banco o registro de datos (Art. 14); derecho de

límites debe comunicarse a otros información sobre su vida privada. (Gutwirth, Serge. Reinventing data protection? 2009.https://search.worldcat.org/es/title/424513781.

[9] El Convenio 108 fue actualizado por la comunidad europea (Convenio 108 +) y fue ratificado por nuestro país recientemente por Ley 27.699.

[10] https://servicios.infoleg.gob.ar/infolegInternet/anexos/315000-319999/318245/norma.htm.

[11] Fallos "Urteaga, Facundo R. c/Estado Mayor Conjunto de las Fuerzas Armadas". Fallós: 321:2767. 15 de octubre de 1998.

actualización y/o rectificación (Art. 16); derecho de supresión del dato falso, erróneo o que ya no debe preservarse (Art. 16).

Estos derechos pueden ejercerse mediante acciones ante la Agencia de Acceso a la Información Pública, órgano de aplicación de la ley, ante los bancos de datos personales públicos o privados destinados a proveer informes a terceros; ante el responsable del tratamiento y almacenamiento de datos personales y la acción de protección de datos personales o habeas data.

Existen distintas sanciones de naturaleza administrativa y penal previstas en normas reglamentarias del organismo, que fueron sistematizadas por la Resolución 126/2024 de la AAIP.

4. Medios de protección preventivos y represivos. Acción preventiva

Ahora bien, fuera del microsistema de la LPDP, encontramos en la actualidad distintos mecanismos de protección de los datos personales.

Así, como arriba lo mencionábamos, el nuevo Código incorporó en el Capítulo 3 del Título I del Libro I, la protección expresa de los derechos personalísimos en sus distintas manifestaciones.

En efecto, luego de reafirmar en el artículo 51 el principio de la inviolabilidad de la persona humana y su dignidad personal, el Código, en su artículo 52 dispone que: "*La persona humana lesionada en su intimidad personal o familiar, honra, o reputación, imagen o identidad, o que de cualquier modo resulte menoscabada en su dignidad personal, puede reclamar la prevención y reparación de los daños sufridos, conforme lo dispuesto en el Libro Tercero, Título V, Capitulo 1*".

El hecho de que el artículo refiera en forma expresa a los derechos personalísimos a la intimidad, imagen, identidad y honor, no obsta a considerar incluidos en esta disposición, otros derechos personalísimos, ya que luego de dicha enumeración, adopta una formula amplia, al referir a la lesión a cualquier modo de menoscabo a la dignidad personal. Sin dudas, el derecho personalísimo al dato personal se encuentra protegido en esta disposición.

Esta última afirmación resulta importante toda vez que el artículo en comentario también incorpora de manera expresa, los medios de protección de los derechos personalísimos, sea en su faz preventiva —tutela inhibitoria— tendiente a conjurar una afectación inminente a derechos personalísimos, como en su faz represiva, tendiente a la reparación de un daño ya causado.

Para la protección eficaz del derecho al dato personal, asume vital relevancia la faz preventiva.

En efecto, el art. 1711 del CCCN prevé la acción preventiva de daños del siguiente modo: *La acción preventiva procede cuando una acción u omisión antijurídica hace previsible la producción de un daño, su continuación o agravamiento. No es exigible la concurrencia de ningún factor de atribución*" (art. 1711).

Como se advierte, este tipo de tutela no exige un factor de atribución de responsabilidad, ya que, si bien tales factores constituyen fundamentos para reconocer la reparación del daño, resultan ajenos a la idea de prevención.

Como lo afirma Wierzba, la idea de reparación ha dejado ya de ser excluyente en materia de responsabilidad civil, en un contexto en el cual no sólo el patrimonio requiere de tutela, sino que se impone una mayor protección de los derechos personalísimos de los individuos.

Este tipo de medio de protección del dato personal resulta muy eficaz dado que habilita al juez a disponer de diversos mecanismos para evitar la continuación o agravamiento de un daño derivado de un mal uso o uso no autorizado, como ordenar el cese de la conservación de un dato de la intimidad, de una imagen, de una localización o ubicación, de la adjudicación de una preferencia, de un prototipo de personalidad, de una identidad u orientación sexual, religiosa, política, etc.

Piénsese como ejemplo en las imágenes y fotografías que se almacenan en una red social. La persona usuaria publica una foto y luego decide borrarla. Ahora bien, eso no significa que la imagen haya desaparecido, dado que, por caso, Instagram o Facebook pueden guardar igual dichas imágenes, dado que cuando aceptamos los términos y condiciones del servicio, hacemos una cesión de propiedad intelectual en favor de la empresa. Por lo que no tenemos certeza que aquello que borramos efectivamente haya desaparecido.

Claramente, se trata de una práctica abusiva por la que se ceden datos en términos de propiedad intelectual; desde el momento que el usuario lo sube deja de ser de propiedad del titular, y pasa a ser de quien lo procesa.

La acción preventiva de daños, se erige como una acción efectiva contra este tratamiento abusivo e ilícito de los datos de las personas.

5. Defensa de los datos personales en el derecho del consumidor

Otros mecanismos de protección de los datos personales los podemos encontrar en el ámbito del derecho del consumidor.

En la actualidad, la cesión de nuestros datos personales, en la mayoría de la población se da a través de la contratación electrónica.

Se trata de contratos de consumo, de adhesión, fuera del establecimiento comercial, celebrados a distancia. (conf. Art 1104 y ss CCCN) Con un simple click, las personas prestan su consentimiento para que el cocontratante acceda a sus datos personales y los incorpore como un activo intangible más de la empresa.

En este contexto, las cláusulas que en la contratación electrónica restrinjan los derechos de los consumidores en la protección de su privacidad y sus datos personales, pueden ser reputadas abusivas. (Conf. Art 1119 CCCN y 37 ley 24.240).

Resulta usual que cuando se aceptan las condiciones generales de contratación —las bases y condiciones— el usuario consiente que sus datos personales pueden ser transmitidos a cualquier otra empresa vinculada, filiales, sucursales, a su sucesora por algún acto corporativo, como la fusión, escisión o transformación.

Como más arriba vimos, tanto el tratamiento como la cesión de los datos personales requieren el consentimiento informado del titular, por lo que una cláusula que suponga la transferencia automática de los datos personales a un tercero sin que el consumidor tenga una instancia de reflexión para autorizar nuevamente el tratamiento de sus datos, constituye una violación al deber de información previsto en el art. 4 de la ley 22.240 y el art. 37 del mismo cuerpo normativo.

Claramente, estas cláusulas que implican cesiones irrestrictas de datos personales suponen grandes riesgos para el titular de los datos personales dado que desconoce de que forma serán tratados sus datos, quienes lo harán, bajo que finalidad, si dichos datos tendrán la debida reserva y finalmente, si se trata de grandes empresas que hacen tráfico transnacional de datos, bajo que jurisdicción podrían eventualmente reclamar.

6. Conclusiones

La protección de los datos personales se erige hoy como uno de los desafíos globales de la hora mas importantes para el derecho actual.

La recopilación, tratamiento y transmisión masiva de metadatos, por distintos actores y para satisfacer distintas finalidades, expone a los titulares a un sinnúmero de riesgos sobre sus derechos fundamentales, sobre todo en tiempos en que la IA diversifica exponencialmente las tareas de procesamiento.

Por ello, sin perjuicio de la necesaria alfabetización digital de los ciudadanos, el rol de los operadores jurídicos resultará clave para que la defensa de este derecho perteneciente al núcleo duro de derechos humanos fundamentales, prevalezca sobre los intereses de los colosos tecnológicos y de los Estados con pretensiones de vigilancia o control social.

Bibliografía

Azar, Aldo. Responsabilidad por los sistemas de inteligencia artificial en entornos virtuales, aplicaciones, sitios de internet y plataformas digitales. TR La Ley AR/DOC/1983/2024.

Basavilbaso, Marina. Régimen argentino de protección de datos personales. La Ley. Revista Código Civil y Comercial de la Nación Año VIII | Número 2 | abril 2022.

Borrelli, Julián C. Acerca de las nuevas tecnologías, su impacto en la protección de datos personales y la ausencia de necesidad de nueva normativa imperativa. TR La Ley AR/ DOC/1096/2025.

Cifuentes, Santos. Reconocimiento jurisprudencial del derecho a los datos personales informáticos y del hábeas data en su verdadero fin tutelar. LA LEY, 1999-E, 151. TR LA LEY AR/DOC/1505/2001.

Cifuentes, Santos Los datos personales informáticos, un derecho autónomo personalísimo. Consecuencias de su reconocimiento y caracterización. TR LA LEY 0003/007394.

De Lorenzo, Miguel Federico Los derechos personalísimos del consumidor en la "cultura de la conectividad": a propósito de la tutela de los datos personales. l Derecho. Edición Especial 21 de septiembre de 2023: Retrospectiva, prospectiva e implementación en el Derecho del Consumidor a 30 años de la Ley N° 24.240.

Faliero, Johanna C. ¿Qué nuevas problemáticas tienen los consumidores en lo referente a la protección y seguridad de sus datos? Año 2023. Cita: MJ-DOC-17288-AR||MJD17288.

Molina Quiroga, Eduardo Protección de datos personales como derecho autónomo. Principios rectores. Informes de solvencia crediticia. Uso arbitrario. Daño moral y material 2003 www.saij.jus.gov.ar Id SAIJ: DACC030027.

Oviedo, Paula. De la protección de los datos personales a la gobernanza. Avances significativos en la región. TR La Ley AR/DOC/976/2023.

Peruzzotti, Mariano. Los 40 años de la democracia de la protección de los datos personales en el derecho argentino. TR La Ley AR/DOC/2648/2023.

Saltor, Carlos Eduardo. Autodeterminación informativa y protección al consumidor en un caso de SIM Swapping. TR La Ley AR/ DOC/1300/2023

Silvester, Pablo. La modernización del derecho de protección de datos personales a nivel global y en argentina. TR La Ley AR/DOC/2385/2023 Sup. Innovación y Derecho 2023.

Wierzba, Sandra. Manual de Obligaciones Civiles y Comerciales según el nuevo CCyCN, Ed. Abeldo Perrot, pág. 259 y sgtes., 2017.

Sobre el autor

Hernán G. Gálvez. Abogado graduado en la Facultad de Ciencias Jurídicas y Sociales de la Universidad Nacional del Litoral. Juez de Primera Instancia Provincia de Santa Fe. Especialista en Derecho de la Empresa y derecho administrativo. Profesor Auxiliar por concurso en Fundamentos de Derecho Privado en la mencionada Casa de Estudios.